СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРИМЕРЕ РОССИЙСКОГО УСТРОЙСТВА.

Панов Р.И.

ФГАОУ ВПО Уральский федеральный университет имени первого Президента России Б.Н.Ельцина ИРИТ-РТФ, Екатеринбург, Россия (620000, Екатеринбург, ул. Мира 32), e-mail: kruft@yandex.ru

В статье рассматривается аналитическое мнение и результаты опросов крупных компаний на предмет ущерба от утечек информации, выяснилось, что почти 90% компаний страдают от утечек информации, не имеют случаев утечки информации, которые могут принести ущерб только 8% компаний. Приведена классификация угроз информационной безопасности, выделены случайные и преднамеренные типы угроз. Рассматриваются последствия исполнения угроз безопасности: разрушение информации, модификация, доступ третьих лиц. Также приведена схема обмена информацией между двумя субъектами с подробным рассмотрением этапов, на которых может быть получен несанкционированный доступ к информации. Приводятся способы защиты от различных угроз на каждом этапе передачи информации. Особое внимание уделено методам аутентификации для получения авторизации доступа к ресурсам системы. Кратко рассматривается новое российское устройство и его уникальные функции в сравнении с существующими криптографическими средствами защиты информации.

Ключевые слова: угрозы безопасности, защита информации, российское устройство.

MODERN DATA PROTECTION METHODS IN RUSSIAN DEVICE AS EXAMPLE.

Panov R.I.

Ural Federal University named after the first President of Russia B. N. Yeltsin, Institute of Radioelectronics and Information Technologies, Yekaterinburg, Russia (620000, Yekaterinburg, street Mira 32), e-mail: kruft@yandex.ru

In this article viewed analytic opinion and company's interview results about damage from information leaks, revealed that near 90% companies suffer from information leaks, only 8% of companies not suffer from leaks. Show information security threats classification, allocated casual and intentional threats types. Show consequences information threats execution: information damage, modify, unauthorized access. Also view information exchange structure between two subjects with detailed description every phase, which contain way for unauthorized access. Observe different ways for protect from any threats in every phase of data transfer. Emphasis paid to authentication methods for authorized access to system resources. Brief observe new Russian device with unique features in compare with existing cryptographic data protection devices.

Key words: security threats, data protection, Russian device.

Введение

В последнее время в СМИ и интернете появляется большое количество сообщений об утечках информации, новых видах вирусов и другой активности в сфере безопасности информационных систем. Более 90% компаний сталкиваются с крупными утечками данных, приводящими к серьёзным финансовым проблемам вплоть до банкротства — такие выводы Zecurion Analytics сделал на основании опроса, проведённого среди компаний, использующих системы защиты информации от утечек.

Аналитики Zecurion провели более 100 интервью с топ-менеджерами компаний и специалистами по кибербезопасности и изучили реальные случаи выявления преднамеренных и случайных утечек корпоративной информации. Выяснилось, что лишь 8%

организаций не страдают от утечек данных, а в 30% компаний крупного и среднего бизнеса фиксируют в среднем по две попытки в месяц похитить ценную информацию, потеря которой сказывается на финансовой стабильности компании. Это подтверждает и максимальный размер ущерба в $30 млн, который понесла российская компания от утечки конфиденциальных данных[5].

В современном мире с большими объёмами информации сталкиваются не только крупные компании, но и рядовые пользователи. Очень часто необходимо производить обмен конфиденциальной информацией с небезопасных компьютеров и по открытым каналам связи с помощью бесплатных почтовых сервисов, таких как gmail, mail.ru и др.

Ни для кого не секрет, что эти сервисы и протоколы безопасности привлекают внимание злоумышленников. В результате уязвимостей в этих протоколах почтовая переписка даже известных политиков может быть открыта вниманию общественности.

На основе исследований случаев воздействия на информацию и несанкционированного доступа к ней можно составить классификацию угроз безопасности, см рис.1

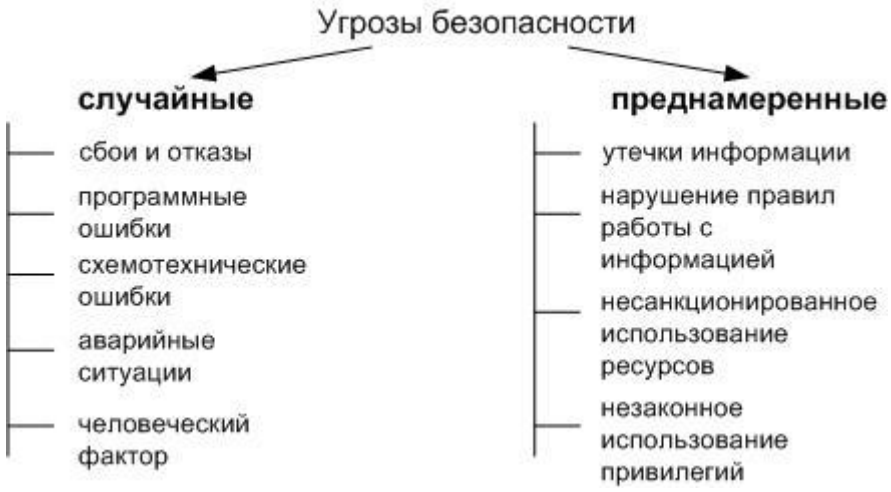

Рис 1. Виды угроз информационной безопасности

Последствиями выполнения угроз безопасности может быть следующее:

1) Разрушение информации
2) Модификация
3) Доступ к информации третьих лиц

Рассмотрим, на каких этапах может быть получен несанкционированный доступ к информации.

Для этого проанализируем пример обмена информацией между пользователями, см рис. 2.

Рис 2. Обмен информацией

П1, П2 – пользователи

У1,У2 – устройства для работы с информацией

Канал передачи – технический канал для обмена информацией.

1) На первом этапе первый пользователь вводит информацию в устройство для её передачи.

На данном этапе получить несанкционированный доступ к информации могут третьи лица следующими способами:

- путём подглядывания
- путём фотографирования клавиатуры на камеру, детектирующую тепловое излучение
- с помощью антенны из соседней комнаты, работающей в паре с анализатором спектра
- с помощью вирусов документирующих нажатые клавиши

Способы защиты: оснащение помещений генераторами шума, выполнение требований безопасности в помещении, использование актуальных антивирусов.

2) На устройстве передачи могут быть установлены средства для защиты информации, различают следующие типы:

- программные (truecrypt, bitlocker)
- аппаратные (datashur, samurai)
- программно-аппаратные (shipka, key_p1, rutoken)

Программные средства позволяют осуществлять аутентификацию пользователей на ПК, шифровать информацию. Существуют аппаратные решения, которые осуществляют автоматическое шифрование информации на съёмные носители после процедуры аутентификации. Программно-аппаратный комплекс устройств повышает безопасность, но также требует аутентификацию.

Аутентификация – процедура проверки подлинности входящего в систему объекта, результатом обычно является авторизация, т.е. предоставление субъекту определенных прав доступа к ресурсам системы.

Процедура аутентификации должна быть максимально защищена, т.к. утечка данных для аутентификации является очень критичной для безопасности.

Существует достаточно много методов аутентификации:

– С помощью PIN кода или пароля

– С помощью одноразовых паролей

– Биометрическая, которая подразделяется на большое количество разных методов аутентификации (отпечаток пальца, геометрия лица, геометрия руки, радужная оболочка глаза, голос, рисунок вен, почерк и т.д.)

– С помощью смарт-карты, USB ключа

– По цифровому сертификату

Работы по созданию новых методов по обеспечению авторизации продолжаются и сегодня, существует и разные экзотические варианты, которые в будущем могут найти своё применение. Например, для прохождения аутентификации может потребоваться правильно расставить фигуры на шахматном поле в соответствии с заданной комбинацией или ввести своё число из большой строки цифр (например, число формируется первой и последней цифрой).

3) На этапе передачи информации по оптоволоконной линии, на съёмных носителях, по радиоканалу или другими способами информация может быть модифицирована, получена третьими лицами или повреждена.

Способы защиты: шифрование передаваемой информации, экранирование линий передачи информации, добавление элементов контроля передаваемых данных.

4) На этапе приёма информации устройством второго пользователя может оказаться, что отправленная первым пользователем информация была изменена или модифицирована, а также повреждена.

Способы защиты: передаваемая информация должна быть зашифрована, для контроля принимаемых данных и проверки их принадлежности отправителю должна быть использована электронно-цифровая подпись файлов, которая позволит не только провести идентификацию отправителя, но и проверить целостность документа.

5) Факторы риска утечки информации и способы защиты на этапе чтения полученной информации вторым пользователем аналогичны этапу 1, за исключением того, что вирусы следят за файлами пользователя, а камера может быть и обычной направленной на монитор.

Перейдём к рассмотрению методов защиты информации, реализованных в новом криптографическом устройстве, вышедшем на российский рынок в конце 2014 года.

Устройство называется Key_P1 Multiclet (допустимое название Ключ_П1), выполнено в виде гаджета с разъёмом USB для подключения к ПК и разъёмами для подключения к устройству USB или SD накопителей. Устройство принадлежит к типу программно-аппаратных, разработано и производится в городе Екатеринбург. На рис. 3 изображена схема подключения устройства в системе защиты информации.

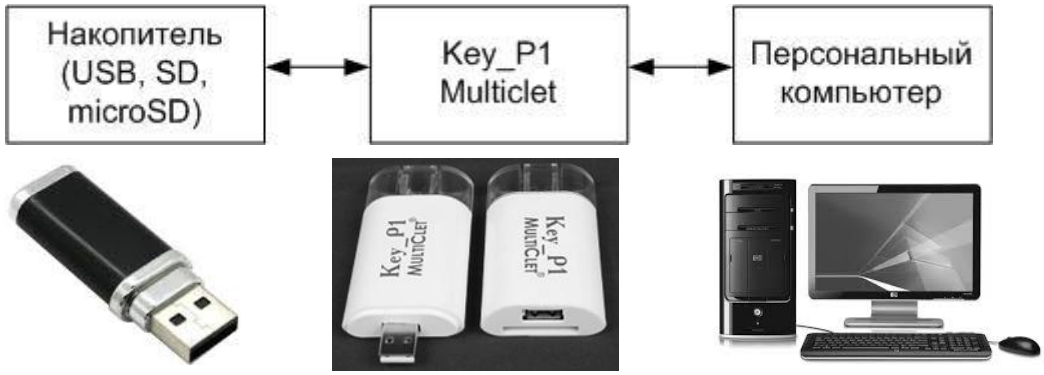

Рис 3. Система работы устройства

Что нового реализовано в данном устройстве защиты информации. Устройство совмещает в себе функционал аппаратных и программных средств.

<u>Уникальный функционал:</u>

1) *Шифрование информации на накопителях*

Шифрование на накопителях информации осуществляется по секторам. Для шифрования на накопителях применяется 1024 ключа, т.е. один файл в зависимости от размера может быть зашифрован несколькими сотнями ключей.

2) *Шифрование информации на ПК*

Шифрование информации, как на ПК, так и на накопителях может осуществляться при помощи синхронных ключей. Это ключи, для которых жёстко установлены алгоритмы формирования на каждом устройстве. Два пользователя, которые хотят обменяться информацией в разных уголках планеты могут обменяться номером алгоритма для формирования ключа и фразой. В результате пользователи создадут на своих устройствах одинаковые ключи и смогут быстро и просто обмениваться защищенной информацией.

3) *Защита от шпионских устройств*

Ни для кого, ни секрет, что в интернете можно недорого купить устройство в виде флешки, которое сможет незаметно для пользователя сыграть в операционной системе роль клавиатуры и мышки и выполнить заданный сценарий (скопировать информацию на накопитель, открыть удаленный доступ к компьютеру жертвы и др.). Устройство Key_P1, разработанное компанией Мультиклет позволяет заблокировать данную вредоносную аппаратуру, выполнив так называемую функцию аппаратного фильтра между ПК и накопителем.

4) *Режим «только чтение»*

Устройство позволяет установить режим «только чтение» при работе с накопителями, таким образом, например в крупной компании, без разрешения администратора безопасности никакая информации с рабочего ПК не будет подвергнута утечке, а также гарантирует защиту флешки от вредоносных программ на ПК. В текущей реализации устройство должно работать в связке с ПО, блокирующим остальные порты USB. Схема работы данного режима приведена на рис 4.

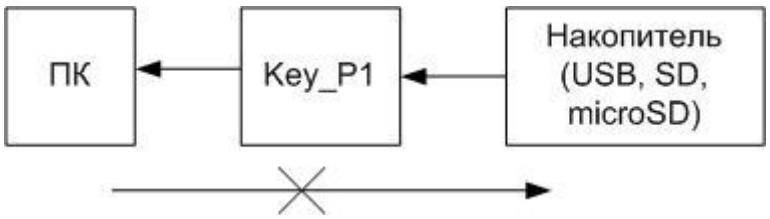

Рис 4. Режим «только чтение»

5) *Режим «только запись»*

Данный режим работы устройства обеспечивает защиту ПК пользователя от возможных вирусов и других вредоносных устройств. Т.е. пользователь не видит содержимое флешки, но может копировать свои данные через устройство Key_P1, которое в свою очередь разместить эти данные в корневом каталоге на съёмном накопителе. Данная функция может быть полезна для съёма информации с дорогостоящего поверенного оборудования, а также для повседневной работы на ПК. Схема работы данного режима приведена на рис 5.

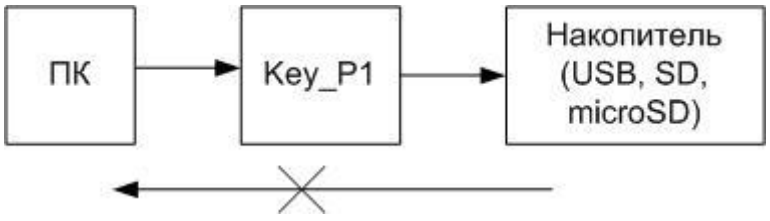

Рис 5. Режим «только запись»

В заключение обзора наиболее интересных функций отечественного криптоустройства отметим факт того, что разработчики сделали шаг по упрощению работы, поскольку установка программного обеспечения на ПК не требуется, и привязки к конкретному ПК также нет.

По моему мнению, устройство для защиты информации, которое станет массовым и «народным» должно обладать следующими чертами:

- Доступность
- Простота и удобство работы
- Мобильность

В заключение отметим, что с каждым годом увеличивается количество утечек информации и в связи с этим фактом растёт и количество устройств по обеспечению информационной безопасности. Серьёзные усилия по защите информации во всём мире начали прикладывать более 20 лет назад.

Существует даже международный день защиты информации, который был учрежден в 1988 году после первой эпидемии сетевого червя, написанного Робертом Моррисом, и отмечается 30 ноября.

Закончить свой доклад хотелось бы показательным фактом истории, которому уже много лет, но актуальность он наверно не потеряет никогда.

Двести лет назад Наполеон проигрывал англичанам Битву при Ватерлоо. По легенде, за сражением внимательно наблюдали Натан и Якоб Ротшильды. Кроме финансовых забот, Ротшильды могли позволить себе лишь одно хобби - почтовых голубей. После битвы голуби были немедленно выпущены с шифрованными инструкциями, привязанными к лапкам. Но Ротшильды не хотели рисковать и, едва убедившись, что Наполеон проигрывает сражение, Натан, загоняя дорогих лошадей, сам мчится в Лондон.
Утром Натан Ротшильд явился на Лондонскую биржу. Он был единственным в Лондоне, кто знал о поражении Наполеона. Сокрушаясь по поводу успехов Наполеона, он немедленно приступил к массовой продаже своих акций. Все остальные биржевики сразу же последовали его примеру, так как решили, что сражение проиграли англичане. Английские, австрийские и прусские ценные бумаги дешевели с каждой минутой и: оптом скупались агентами Ротшильда. О том, что Наполеон проиграл битву, на бирже узнали лишь через день. Многие держатели ценных бумаг покончили с собой, а Натан заработал 40 миллионов

фунтов стерлингов. Реальная информация, полученная раньше других, позволила Ротшильдам вести беспроигрышную игру на бирже. Ротшильды не только придумали знаменитую фразу "Кто владеет информацией, тот владеет миром", они подготовили все, чтобы информация попадала в первую очередь к ним." [4]

Пример показателен тем, что информацию получили адресаты, и дошла она в неискаженном виде, понятном только тем, кому она была направлена.

Лучший доклад по итогам конференции «Информационные технологии, телекоммуникации и системы управления»

Список литературы

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова//Технические средства и методы защиты информации:Учебник для вузов / – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

2. Сабанов А. Обзор технологий идентификации и аутентификации, конф. АДЭ №7 (сентябрь 2006) URL: https://aladdin-rd.ru/company/pressroom/articles/9129/?sphrase_id=361472

3. (дата обращения: 10.12.2014)

4. Современные биометрические методы идентификации //Информационный портал Хабрахабр (11 августа 2011): сайт - URL: http://habrahabr.ru/post/126144/

5. (дата обращения: 10.12.2014)

6. Краюхин Д. Кто владеет информацией – тот владеет миром //Рубрика Права человека (30 октября 2012): сайт - URL: http://7x7-journal.ru/post/21905

7. (дата обращения: 10.12.2014)

8. Zecurion Analytics: российские компании теряют до $30 млн из-за утечек данных

9. человека (28 октября 2014): сайт - URL: http://www.zecurion.ru/press/5099/